REMARKS

The drawings are now labeled correctly with "New Sheet" in the top margin of each page.

The Abstract was found objectionable because of its length, and has been amended above. Corrections to the specification have also been made above, including "spelling-out" acronyms as requested by the Examiner No new matter has been added.

Claims 4 and 19 were found objectionable because "DMZ" was not spelled out, and correction has been made above.

Claims 1-2, 16-17 and 21-22 were found objectionable because the term "userID" was not spelled out. Applicants respectfully traverse this rejection because "userID" is a well known term, better known than the spelled out terminology "user identification". The specification has been amended to "spell-out" the term "userID".

Claims 1-22 were rejected under 35 USC 102 based on Whipple. Claims 8-10 and 15 have been canceled aboved. New claims 23-26 have been added. Applicants respectfully traverse this rejection as applied to amended claims 1-7, 9-14 and 16-22 and new claims 23-26, based on the following.

Amended claim 1 recites a method for authenticating a first user in a protected network to an application shared concurrently with a second user in an unprotected network. The first user supplies a userID and a password to a first server within the protected network for authentication for the application. The application resides in a third network configured as a buffer between the protected network and the unprotected network. The user's password is not sent from the protected network into the third network to access the application. The first server determines that the userID and password are authentic. In response, the first server forwards to the application an authentication key for the first user and a selection by the first user pertaining to the application. The application determines that the key is authentic. In response, the application complies with the selection by the first user. The second user supplies another userID and another password to the application. The application determines that the other

userID and the other password are authentic, and in response, the application complies with a selection made by the second user pertaining to the application.

Thus, according to claim 1, the first server within the protected network forwards to the application in the buffer network an authentication key for the first user. Consequently, the password of the first user need not be and is not sent into the buffer network to access the application. Therefore, the user's password cannot be discovered by a hacker with access only to the buffer network. Also according to claim 1, a second user in the unprotected network sends its userID and password to the application in the buffer network for authentication, so the application supports authentication in two different manners. In contrast to claim 1, Whipple et al. teach that a user 58 (Figure 8) on the WWW, i.e. **in an unprotected network** sends a key to a web server to access a secure collaborative workspace 54 in a DMZ network. However, it is clear that computer 58 of Whipple et al. is in the unprotected Internet because the caption in the drawing for computer 58 is "web enterprise", the communication protocol is "HTTP" which is a WWW protocol, and computer 58 communicates to a "web server" 60 in the DMZ. This is substantially different from claim 1 of the present invention where the server **in the protected network** uses a key to authenticate a user in the protected network to the application in the buffer network. As for communications received by secure collaborative workspace 54 in the DMZ from Hub Enterprise 50 in Whipple et al., there is no indication or disclosure that this uses a key for authentication. Therefore, in contrast to claim 1, Whipple et al. do not teach or suggest that a password of a person **in a protected network** is not sent to a buffer network to prevent a hacker in an unprotected network with access to the buffer network from learning the password from the buffer network. Instead, according to claim 1, the user in the protected network authenticates himself or herself with a userID and password to a server in the protected network, and in response, the server in the protected network furnishes an authentication key (and a selection made by the user pertaining to the application) to the application in the buffer network to authenticate the user to the application in the buffer network. Therefore, the rejection under 35 USC 102 based on Whipple et al. should be withdrawn, and no rejection under 35 USC 103 should be made.

Claims 2-7 and 11-14 depend on claim 1, and therefore distinguish over the prior art for the same reasons as claim 1.

Independent claim 16 distinguishes over the prior art for the same reasons that claim 1 distinguishes thereover. Claims 17-20 depend on claim 16, and therefore distinguish over the prior art for the same reasons as claim 1.

Independent claim 21 distinguishes over the prior art for the same reasons that claim 1 distinguishes thereover. Claim 22 depends on claim 21, and therefore distinguishes over the prior art for the same reasons as claim 1.

Independent claim 23 distinguishes over the prior art for similar reasons that claim 1 distinguishes thereover. Claims 24-26 depend on claim 23, and therefore distinguish over the prior art for the same reasons as claim 1.

Based on the foregoing, the present patent application as amended above should be allowed.

Respectfully submitted,

Dated: 02/05/2007
Telephone: 607-429-4368
Fax No.: 607-429-4119

/Arthur J. Samodovitz/
Arthur J. Samodovitz
Reg. No. 31,297